Handbuch Desktop Management

Business Desktops

Dokument-Teilenummer: 312947-042

September 2003

Dieses Handbuch enthält Definitionen und Anleitungen zur Verwendung der Sicherheitsfunktionen und der Intelligent Manageability, die bei bestimmten Modellen voreingestellt sind.

⚠ **VORSICHT:** In dieser Form hervorgehobener Text weist darauf hin, dass die Nichtbeachtung zu Verletzungen oder zum Tod führen kann.

⚠ **ACHTUNG:** In dieser Form gekennzeichneter Text weist auf eine Anleitung hin, deren Nichtbeachtung zur Beschädigung von Komponenten oder zum Verlust von Daten führen kann.

Handbuch Desktop Management
Business Desktops

Zweite Ausgabe (September 2003)
Dokument-Teilenummer: 312947-042

Inhalt

Handbuch Desktop Management

Index

Handbuch Desktop Management

HP Intelligent Manageability bietet standardbasierte Lösungen zur Verwaltung und Steuerung von Desktops, Workstations und Notebook-PCs in einer Netzwerkumgebung. HP war 1995 mit der Einführung der branchenweit ersten vollständig verwaltbaren Desktop-PCs ein Vorreiter im Bereich der Desktop Manageability. Die Manageability-Technologie von HP ist patentrechtlich geschützt. Seither steht HP an der Spitze eines branchenweiten Bemühens, die für den effektiven Einsatz sowie die Konfiguration und Verwaltung von Desktops, Workstations und Notebook-PCs erforderlichen Standards und Infrastrukturen zu entwickeln. HP arbeitet eng mit marktführenden Anbietern von Management-Software-Lösungen zusammen, um die Kompatibilität zwischen Intelligent Manageability und diesen Produkten sicherzustellen. Intelligent Manageability ist ein wichtiger Aspekt des umfassenden Engagements von HP, Ihnen PC Lifecycle-Lösungen für alle vier Phasen des Lebenszyklus eines Desktop-PCs anzubieten – von der Planung und dem Einsatz über die Verwaltung bis zur Umstellung.

Hauptfunktionen und -merkmale von Desktop Management:

- Erste Konfiguration und erster Einsatz
- Remote System Installation
- Software-Aktualisierung und -Management
- ROM-Flash
- Bestandsüberwachung und Sicherheit
- Fehlermeldung und Fehlerbeseitigung

Die Unterstützung spezieller, in diesem Handbuch beschriebener Funktionen kann sich je nach Modell oder Software-Version unterscheiden.

Erste Konfiguration und erster Einsatz

Der Computer wird mit vorinstalliertem Systemsoftware-Image geliefert. Nach einem kurzen Vorgang des „Auspackens“ der Software ist der Computer einsatzbereit.

Möglicherweise ziehen Sie es vor, das vorinstallierte Software-Image durch eine benutzerdefinierte System- und Anwendungssoftware zu ersetzen. Es gibt mehrere Methoden zum Ersetzen eines benutzerdefinierten Software-Images. Folgende Methoden können verwendet werden:

- Installation zusätzlicher Software-Anwendungen nach dem Auspacken des vorinstallierten Software-Images
- Verwendung von Software-Einsatz-Tools, wie etwa Altiris Deployment Solution™, um die vorinstallierte Software durch ein benutzerdefiniertes Software-Image zu ersetzen
- Verwendung eines Disk-Kopiervorgangs zum Kopieren des Inhalts einer Festplatte auf eine andere

Welches Einsatzverfahren am besten geeignet ist, hängt von Ihrer IT-Umgebung und den damit verbundenen Prozessen ab. Der Abschnitt zum PC-Einsatz auf der HP Website zu Lifecycle-Lösungen (http://h18000.www1.hp.com/solutions/pcsolutions) bietet Ihnen Informationen zur Auswahl des besten Verfahrens.

Die *Compaq Restore!* CD, das ROM-basierte Setup und die Hardware mit ACPI-Unterstützung bieten zusätzliche Hilfe bei der Wiederherstellung der Systemsoftware, dem Konfigurations-Management, der Fehlerbeseitigung sowie bei der Energieverwaltung.

Remote System Installation

Remote System Installation erlaubt Ihnen, Ihr System mit Hilfe der Software und der Konfigurationsinformationen von einem Netzwerk-Server zu starten und zu installieren. Hierfür wird das Preboot Execution Environment (PXE) gestartet. Die Remote-Installationsfunktion wird normalerweise als Tool zur Systemeinrichtung und -konfiguration verwendet und kann darüber hinaus für die folgenden Aufgaben eingesetzt werden:

- Formatieren einer Festplatte
- Einsetzen eines Software-Images auf einem oder mehreren neuen PCs
- Remote-Aktualisierung des System-BIOS im Flash-ROM („Remote-ROM-Flash“ auf Seite 8)
- Konfigurieren der Einstellungen im System-BIOS

Drücken Sie die Taste **F12**, um Remote System Installation zu starten, wenn die Meldung **F12 = Network Service Boot** (Starten über Netzwerk) in der unteren rechten Ecke der HP Logoanzeige erscheint. Folgen Sie den Anleitungen auf dem Bildschirm, um fortzufahren. Die standardmäßige Boot-Reihenfolge kann im BIOS konfiguriert und so geändert werden, dass immer zunächst ein PXE-Boot durchgeführt wird.

HP und Altiris, Inc. stellen gemeinsam Tools zur Verfügung, die den Einsatz und das Management von Firmen-PCs vereinfachen, weniger zeitaufwendig gestalten, die Total Cost of Ownership senken und die HP PCs zu den Client-PCs mit der besten Manageability in Unternehmen machen.

Software-Aktualisierung und -Management

HP bietet verschiedene Tools für Software-Aktualisierung und -Management auf Desktop-Computern und Workstations: Altiris; Altiris PC Transplant Pro; HP Client Manager Software, eine Altiris Lösung; System Software Manager; Proactive Change Notification und ActiveUpdate.

HP Client Manager Software

Intelligent HP Client Manager Software (HP CMS) integriert die HP Intelligent Manageability-Technologie innerhalb von Altiris und bietet so erstklassige Hardware-Management-Funktionen für HP Zugangsgeräte, wie z. B.:

- Ausführliche Ansichten des Hardware-Inventars für die Bestandsverwaltung
- Überwachung des PC-Zustands und Diagnose
- Proaktive Benachrichtigung über Änderungen in der Hardware-Umgebung
- Über das Web zugängliche Berichtserstellung von wichtigen Detailinformationen, wie beispielsweise Warnmeldungen bei Geräteüberhitzung, mangelndem Speicherplatz usw.
- Remote-Aktualisierung von Systemsoftware, wie beispielsweise Gerätetreiber und ROM-BIOS
- Remote-Änderung der Boot-Reihenfolge

Weitere Informationen zu HP Client Manager finden Sie unter http://h18000.www1.hp.com/im/client_mgr.html.

Altiris Lösungen

HP Client Management Solutions ermöglichen ein zentrales Hardware-Management von HP Client-Geräten für alle Abschnitte im IT-Lebenszyklus.

- Bestandsverwaltung
  - ❏ Konformität mit SW-Lizenzen
  - ❏ PC-Protokollierung und -Berichtserstellung
  - ❏ Leasingvertrag, Bestandsüberwachung

- Einsatz und Migration
  - Migration von Microsoft Windows 2000, Windows XP Professional oder Home Edition
  - Systemeinrichtung
  - Migration
- Help Desk und Problemlösung
  - Management von Help Desk-Tickets
  - Remote-Fehlerbehebung
  - Remote-Problemlösung
  - Wiederherstellung nach einem Client-Ausfall
- Software und Operations Management
  - Kontinuierliches Desktop Management
  - Einrichtung von HP Systemsoftware
  - Automatische Anwendungswiederherstellung

Das vorinstallierte Image ausgewählter Desktop- und Notebook-Modelle beinhaltet einen Altiris Management Agent. Dieser Agent ermöglicht die Kommunikation mit der Altiris Development Solution, welche zur Einrichtung neuer Hardware oder zur Migration auf ein neues Betriebssystem mit Hilfe einfacher Assistenten verwendet werden kann. Altiris Lösungen bieten benutzerfreundliche Software-Verteilungsmöglichkeiten. Wenn Altiris in Verbindung mit System Software Manager oder HP Client Manager verwendet wird, kann der Administrator zudem den ROM-BIOS und die Gerätetreiber aktualisieren.

Weitere Informationen finden Sie unter http://www.hp.com/go/easydeploy.

Altiris PC Transplant Pro

Altiris PC Transplant Pro ermöglicht eine problemlose PC-Migration, indem alte Einstellungen, Voreinstellungen und Daten erhalten bleiben und auf schnelle und einfache Weise in die neue Umgebung überstellt werden. Anstelle von Stunden oder sogar Tagen dauert dieser Vorgang nur wenige Minuten, und schon können Sie mit Ihrem Desktop-Computer in gewohnter Weise arbeiten.

Weitere Informationen zum Download einer voll funktionsfähigen, 30 Tage gültigen Testversion erhalten Sie unter http://h18000.www1.hp.com/im/prodinfo.html#deploy.

System Software Manager

System Software Manager (SSM) ist ein Dienstprogramm, mit dem Software auf Systemebene auf mehreren Systemen gleichzeitig aktualisiert werden kann. Wenn SSM auf einem PC-Client-System ausgeführt wird, erkennt es sowohl Hardware- als auch Software-Versionen und aktualisiert die betreffende Software dann von einem zentralen Repository, dem so genannten Dateispeicher, aus. Treiberversionen, die von SSM unterstützt werden, sind auf der Website zum Herunterladen von Treibern sowie auf der Support Software CD durch ein spezielles Symbol gekennzeichnet. Besuchen Sie zum Herunterladen des Dienstprogramms oder zum Abrufen weiterer Informationen zu SSM die folgende Website: http://h18000.www1.hp.com/im/ssmwp.html.

Proactive Change Notification

Das Programm Proactive Change Notification versendet auf Basis der Eintragungen auf der Website Subscriber's Choice proaktiv und automatisch folgende Mails:

- Eine PCN-E-Mail (Proactive Change Notification), in der Sie bis zu 60 Tage im Voraus über Änderungen an der Hard- und Software an den meisten Computern und Servern für Unternehmen informiert werden.
- Eine E-Mail mit Informationen, Ratschlägen und Hinweisen für Kunden, Sicherheitsmitteilungen und Treiber-Warnmeldungen für die meisten Computer und Server für Unternehmen.

Durch die Erstellung Ihres persönlichen Profils wird gewährleistet, dass Sie nur Informationen erhalten, die für eine spezifische IT-Umgebung von Interesse sind. Weitere Informationen zu dem Programm Proactive Change Notification und zur Erstellung benutzerdefinierter Profile erhalten Sie unter http://www.hp.com/go/pcn.

ActiveUpdate

ActiveUpdate ist eine Client-basierte Anwendung von HP. Der ActiveUpdate Client wird auf dem lokalen System ausgeführt und verwendet ein benutzerdefiniertes Profil, um Software-Aktualisierungen für die meisten Computer und Server für Unternehmen von HP proaktiv und automatisch herunterzuladen. Diese Software-Aktualisierungen können auf dem Computer, für den sie von HP Client Manager Software und System Software Manager vorgesehen sind, intelligent eingerichtet werden.

Weitere Informationen zu ActiveUpdate sowie zum Herunterladen der Anwendung und zum Erstellen eines benutzerdefinierten Profils finden Sie unter folgender Adresse: http://h18000.www1.hp.com/products/servers/management/activeupdate/index.html.

ROM-Flash

Der Computer verfügt über einen programmierbaren Flash- ROM-Speicher (ROM=Read Only Memory, Nur-Lese-Speicher). Wenn Sie ein Setup-Kennwort in Computer Setup (F10) Utility einrichten, können Sie verhindern, dass der ROM-Speicher unbeabsichtigt aktualisiert oder überschrieben wird. Dies ist wichtig zur Gewährleistung des fehlerfreien Betriebs des Computers. Wenn Sie den ROM-Speicher aktualisieren müssen oder möchten, können Sie wie folgt vorgehen:

- Bestellen Sie eine aktuelle ROMPaq Diskette von HP.
- Laden Sie die aktuellen ROMPaq-Images unter http://h18000.www1.hp.com/im/ssmwp.html herunter.

ACHTUNG: Für den maximalen Schutz des ROM-Speichers müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert die unbefugte Aktualisierung des ROM-Speichers. Mit Hilfe von System Software Manager kann der Systemadministrator das Setup-Kennwort auf mehreren PCs gleichzeitig einstellen. Weitere Informationen finden Sie unter folgender Adresse: http://h18000.www1.hp.com/im/ssmwp.html.

Remote-ROM-Flash

Remote ROM Flash ermöglicht dem Systemadministrator, den ROM-Speicher von HP Computern direkt von der zentralen Netzwerk-Management-Konsole aus auf sichere Art und Weise zu aktualisieren. Da der Systemadministrator diese Aufgabe für mehrere Computer und PCs remote durchführen kann, ergibt sich dadurch ein konsistenter Einsatz und eine bessere Überwachung von HP PC ROM-Images über das Netzwerk. Dies führt außerdem zu höherer Produktivität und niedrigeren Total Cost of Ownership.

Der Computer muss eingeschaltet sein oder über die Remote Wakeup-Funktion eingeschaltet werden, wenn Remote ROM Flash verwendet wird.

Weitere Informationen zum Remote ROM Flash erhalten Sie in der HP Client Manager Software oder im System Software Manager unter http://h18000.www1.hp.com/im/prodinfo.html.

HPQFlash

Mit dem Dienstprogramm HPQFlash kann der System-ROM auf einzelnen PCs über das Windows Betriebssystem lokal aktualisiert oder wiederhergestellt werden.

Weitere Informationen zu HPQFlash erhalten Sie unter http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18607.html.

FailSafe Boot Block ROM

FailSafe Boot Block ROM ermöglicht eine Wiederherstellung des Systems im unwahrscheinlichen Fall eines ROM-Flash-Fehlers, z. B. bei einem Stromausfall während einer ROM-Aktualisierung. Der Boot-Block ist ein flash-geschützter Bereich des ROM-Speichers, der jedes Mal die Gültigkeit des ROM-Flash-Speichers überprüft, wenn der Computer eingeschaltet wird.

- Wenn der ROM-Speicher des Systems gültig ist, startet das System normal.
- Wenn der ROM-Speicher den Gültigkeitstest nicht besteht, bietet FailSafe Boot Block ROM ausreichend Unterstützung, damit das System von einer ROMPaq Diskette aus starten kann, die dem ROM-Speicher ein gültiges Image zuweist.

Wenn im Boot-Block ein ungültiger System-ROM-Speicher festgestellt wird, leuchtet die ROTE Betriebs-LED achtmal im Abstand von jeweils einer Sekunde, mit einer zweisekündigen Pause. Gleichzeitig wird auch ein achtfacher Signalton ausgegeben. Eine Meldung wird angezeigt, die angibt, dass das System in den Boot-Block-Wiederherstellungsmodus schaltet (modellabhängig).

Wenn Sie das System wiederherstellen möchten, nachdem es in den Boot-Block-Wiederherstellungsmodus geschaltet hat, führen Sie folgende Schritte aus:

1. Wenn sich eine Diskette im Laufwerk befindet, nehmen Sie diese aus dem Laufwerk, und schalten Sie den Computer aus.
2. Legen Sie eine ROMPaq Diskette in das Diskettenlaufwerk ein.
3. Schalten Sie den Strom wieder ein.
4. Wenn keine ROMPaq Diskette gefunden wird, werden Sie aufgefordert, diese Diskette einzulegen und den Computer neu zu starten.
5. Wenn ein Setup-Kennwort eingerichtet wurde, leuchtet die LED-Anzeige der **Feststelltaste**, und Sie werden zur Eingabe des Kennworts aufgefordert.
6. Geben Sie das Setup-Kennwort ein.

7. Wenn das System erfolgreich von der Diskette startet und den ROM erfolgreich umprogrammiert, beginnen die drei LED-Anzeigen auf der Tastatur zu leuchten. Eine lauter werdende Abfolge von akustischen Signalen kennzeichnet zusätzlich den erfolgreichen Abschluss des Vorgangs.
8. Nehmen Sie die Diskette aus dem Laufwerk, und schalten Sie den Computer aus.
9. Starten Sie den Computer anschließend neu.

Die folgende Tabelle gibt einen Überblick über die von Boot Block ROM verwendeten verschiedenen Kombinationen der LED-Anzeigen auf der Tastatur (insofern eine PS/2-Tastatur angeschlossen ist) und ihre Bedeutungen sowie die Schritte in Verbindung mit diesen Kombinationen.

Von Boot Block ROM verwendete Kombinationen der LED-Anzeigen auf der Tastatur

Modus FailSafe Boot Block	Tastatur LED-Farbe	Tastatur LED-Aktivität	Zustand/Meldung
Num	Grün	Ein	ROMPaq Diskette nicht vorhanden oder fehlerhaft oder Laufwerk nicht bereit.
Feststelltaste	Grün	Ein	Kennwort eingeben.
Num, Feststelltaste, Rollen	Grün	Blinkt nacheinander – N, C, SL	Tastatur im Netzwerkmodus gesperrt.
Num, Feststelltaste, Rollen	Grün	Ein	Boot Block ROM-Flash erfolgreich. Schalten Sie den Computer aus und anschließend wieder ein, um neu zu starten.

✎ Auf USB-Tastaturen wird die Diagnosefunktion der Tastatur-LEDs nicht unterstützt.

Replizieren des Setups

Die folgenden Verfahren ermöglichen dem Systemadministrator, ohne großen Aufwand eine Setup-Konfiguration auf andere Computer des gleichen Modells zu kopieren. Auf diese Weise kann die Konfiguration mehrerer Computer schneller und mit größerer Einheitlichkeit durchgeführt werden.

Für beide Verfahren benötigen Sie ein Diskettenlaufwerk oder ein unterstütztes USB-Flash-Media-Gerät, z. B. den HP USB Memory Key.

Kopieren auf einen Computer

ACHTUNG: Die Setup-Konfiguration ist modellabhängig. Wenn das Modell von Quell- und Zielcomputer nicht übereinstimmt, wird unter Umständen das Dateisystem beschädigt. Die Setup-Konfiguration eines D510 Ultra-Slim Desktop darf beispielsweise nicht auf einen D510 E-PC kopiert werden.

1. Wählen Sie die gewünschte Setup-Konfiguration aus. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige am Monitor grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Legen Sie eine Diskette oder ein USB-Flash-Media-Gerät ein.
4. Klicken Sie auf **File > Save to Diskette** (Datei > Auf Diskette speichern). Führen Sie die am Bildschirm angezeigten Anleitungen aus, um die Konfigurationsdiskette oder das USB-Flash-Media- Gerät zu erstellen.
5. Schalten Sie den zu konfigurierenden Computer aus, und legen Sie die Konfigurationsdiskette bzw. das USB-Flash-Media-Gerät ein.

6. Schalten Sie den zu konfigurierenden Computer ein. Drücken Sie die Taste **F10**, sobald die LED-Anzeige am Monitor grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.
7. Klicken Sie auf **File > Restore from Diskette** (Datei > Von Diskette wiederherstellen), und folgen Sie den Anleitungen auf dem Bildschirm.
8. Starten Sie den Computer nach Abschluss der Konfiguration neu.

Kopieren auf mehrere Computer

ACHTUNG: Die Setup-Konfiguration ist modellabhängig. Wenn das Modell von Quell- und Zielcomputer nicht übereinstimmt, wird unter Umständen das Dateisystem beschädigt. Die Setup-Konfiguration eines D510 Ultra-Slim Desktop darf beispielsweise nicht auf einen D510 E-PC kopiert werden.

Bei dieser Methode nimmt die Erstellung der Konfigurationsdiskette bzw. des USB-Flash-Media-Geräts ein wenig mehr Zeit in Anspruch, das Kopieren der Konfiguration auf die Zielcomputer wird jedoch erheblich beschleunigt.

Unter Windows 2000 kann keine bootfähige Diskette erstellt werden. Für dieses Verfahren bzw. für die Erstellung eines bootfähigen USB-Flash-Media-Geräts wird jedoch eine bootfähige Diskette benötigt. Wenn für die Erstellung einer bootfähigen Diskette weder Windows 9x noch Windows XP verfügbar ist, können Sie das Verfahren für die Kopie auf einen Computer verwenden (siehe „Kopieren auf einen Computer“ auf Seite 11).

1. Erstellen Sie eine bootfähige Diskette oder ein USB-Flash-Media-Gerät. Siehe „Bootfähige Diskette“ auf Seite 14, „Unterstützte USB-Flash-Media-Geräte“ auf Seite 14 oder „Nicht unterstützte USB-Flash-Media-Geräte“ auf Seite 18.

ACHTUNG: Nicht alle Computer können über ein USB-Flash-Media-Gerät gestartet werden. Wenn in der standardmäßigen Boot-Reihenfolge im Computer Setup (F10) Utility das USB-Gerät vor der Festplatte aufgelistet wird, kann der Computer über ein USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

2. Wählen Sie die gewünschte Setup-Konfiguration aus. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie unter Windows auf **Start > Beenden > Neu starten**.
3. Drücken Sie die Taste **F10**, sobald die LED-Anzeige am Monitor grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

4. Legen Sie die bootfähige Diskette bzw. das USB-Flash-Media-Gerät ein.
5. Klicken Sie auf **File > Save to Diskette** (Datei > Auf Diskette speichern). Führen Sie die am Bildschirm angezeigten Anleitungen aus, um die Konfigurationsdiskette oder das USB-Flash-Media-Gerät zu erstellen.
6. Laden Sie ein BIOS-Dienstprogramm zum Replizieren des Setups herunter (repset.exe), und kopieren Sie es auf die Konfigurationsdiskette oder das USB-Flash-Media-Gerät. Das Dienstprogramm erhalten Sie unter http://h18000.www1.hp.com/support/files/hpcpqdt/us/download/18040.html.
7. Erstellen Sie auf der Konfigurationsdiskette bzw. auf dem USB-Flash-Media-Gerät eine Datei „autoexec.bat“ mit folgendem Befehl:

   repset.exe
8. Schalten Sie den zu konfigurierenden Computer aus. Legen Sie die Konfigurationsdiskette bzw. das USB-Flash-Media-Gerät ein, und schalten Sie den Computer ein. Das Konfigurationsdienstprogramm wird automatisch ausgeführt.
9. Starten Sie den Computer nach Abschluss der Konfiguration neu.

Erstellen eines bootfähigen Geräts

Bootfähige Diskette

Diese Anleitung bezieht sich auf Windows XP Professional und Home Edition. Die Erstellung bootfähiger Disketten wird von Windows 2000 nicht unterstützt.

1. Legen Sie eine Diskette in das Diskettenlaufwerk ein.
2. Klicken Sie auf **Start** und anschließend auf **Arbeitsplatz**.
3. Klicken Sie mit der rechten Maustaste auf das Diskettenlaufwerk, und wählen Sie **Formatieren** aus.
4. Aktivieren Sie das Kontrollkästchen **MS-DOS-Startdiskette erstellen**, und klicken Sie anschließend auf **Start**.

Fahren Sie mit „Kopieren auf mehrere Computer“ auf Seite 12 fort.

Unterstützte USB-Flash-Media-Geräte

Unterstützte Geräte, z. B. der HP USB Memory Key oder DiskOnKey, verfügen über ein vorinstalliertes Image, welches die Nutzung als bootfähiges Gerät vereinfacht. Verwenden Sie die später in diesem Kapitel beschriebene Verfahren, wenn der verwendete USB Memory Key kein solches Image aufweist (siehe „Nicht unterstützte USB-Flash-Media-Geräte“ auf Seite 18).

ACHTUNG: Nicht alle Computer können über ein USB-Flash-Media-Gerät gestartet werden. Wenn in der standardmäßigen Boot-Reihenfolge im Computer Setup (F10) Utility das USB-Gerät vor der Festplatte aufgelistet wird, kann der Computer über ein USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

Für die Erstellung eines bootfähigen USB-Flash-Media-Geräts benötigen Sie Folgendes:

- Eines der folgenden Systeme:
  - Compaq Evo D510 Ultra-Slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor
  - HP Compaq Business Desktop D530 Serie – Ultra-Slim Desktop, Small Form Factor oder Convertible Minitower
  - Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c oder N1000c Notebooks
  - Compaq Presario 1500 oder 2800 Notebooks

  Je nach BIOS unterstützen teilweise auch künftige Systeme Boot-Vorgänge über den HP USB Memory Key.

ACHTUNG: Wenn Sie einen anderen als die oben erwähnten Computer verwenden, sollten Sie sich vergewissern, dass in der standardmäßigen Boot-Reihenfolge im Computer Setup (F10) Utility das USB-Gerät vor der Festplatte genannt wird.

- Eines der folgenden Speichermodule:
  - HP USB Memory Key mit 16 MB
  - HP USB Memory Key mit 32 MB
  - DiskOnKey mit 32 MB
  - HP USB Memory Key mit 64 MB
  - DiskOnKey mit 64 MB
  - HP USB Memory Key mit 128 MB
  - DiskOnKey mit 128 MB
- Eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS. Wenn SYS nicht verfügbar ist, kann auch FORMAT verwendet werden. Es gehen jedoch alle vorhandenen Dateien auf dem USB Memory Key verloren.

1. Schalten Sie den Computer aus.
2. Schließen Sie den USB Memory Key an einen der USB-Anschlüsse des Computers an, und entfernen Sie alle anderen USB-Speichergeräte außer den USB-Diskettenlaufwerken.

3. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie den Computer ein, um diesen über die DOS-Diskette zu starten.
4. Führen Sie an der Eingabeaufforderung A:\ FDISK aus, indem Sie **FDISK** eingeben und die Eingabetaste drücken. Klicken Sie an der Eingabeaufforderung auf **Yes** (**Y**), um die Unterstützung großer Disketten zu aktivieren.
5. Geben Sie Ihre Auswahl [**5**] ein, um die Laufwerke im System anzuzeigen. Als USB Memory Key wird das Laufwerk verwendet, das mit der Größe eines der angegebenen Laufwerke weitgehend übereinstimmt. Zumeist handelt es sich um das letzte Laufwerk in der Liste. Notieren Sie den Laufwerkbuchstaben.

   Laufwerk für den USB Memory Key: _____

ACHTUNG: Fahren Sie nicht fort, wenn kein Laufwerk mit dem USB Memory Key übereinstimmt. Andernfalls könnten Daten verloren gehen. Überprüfen Sie alle USB-Anschlüsse auf zusätzliche Speichergeräte. Entfernen Sie möglicherweise vorhandene Speichergeräte, starten Sie den Computer neu, und fahren Sie mit Schritt 4 fort. Sind keine anderen Speichergeräte vorhanden, unterstützt das System den USB Memory Key nicht oder der USB Memory Key ist defekt. Fahren Sie in diesem Fall NICHT mit dem Vorgang fort.

6. Beenden Sie FDISK und kehren Sie zur Eingabeaufforderung A:\ zurück, indem Sie die Taste **Esc** drücken.
7. Fahren Sie mit Schritt 8 fort, wenn die bootfähige DOS-Diskette SYS.COM beinhaltet. Andernfalls fahren Sie mit Schritt 9 fort.
8. Geben Sie an der Eingabeaufforderung A:\ **SYS x:** ein. Das x steht in diesem Fall für den oben notierten Laufwerksbuchstaben. Fahren Sie mit Schritt 13 fort.

ACHTUNG: Vergewissern Sie sich, dass Sie den korrekten Laufwerksbuchstaben für den USB Memory Key eingegeben haben.

   Nachdem die Systemdateien übertragen wurden, kehrt SYS zur Eingabeaufforderung A:\ zurück.

9. Kopieren Sie alle Dateien auf dem USB Memory Key, die beibehalten werden sollen, in ein temporäres Verzeichnis auf einem anderen Laufwerk (z. B. auf die interne Festplatte des Systems).
10. Geben Sie an der Eingabeaufforderung A:\ **FORMAT /S X:** ein. Das x steht in diesem Fall für den oben notierten Laufwerksbuchstaben.

ACHTUNG: Vergewissern Sie sich, dass Sie den korrekten Laufwerksbuchstaben für den USB Memory Key eingegeben haben.

Durch FORMAT werden eine oder mehrere Warnungen angezeigt, in denen Sie die Fortführung des Vorgangs bestätigen müssen. Geben Sie bei jeder Warnung **y** ein. Der Befehl FORMAT formatiert den USB Memory Key, fügt die Systemdateien hinzu und fordert eine Datenträgerbezeichnung an.

11. Drücken Sie die **Eingabetaste**, um keine Bezeichnung anzugeben, oder geben Sie einen Namen ein.
12. Kopieren Sie die in Schritt 9 gespeicherten Dateien auf den USB Memory Key.
13. Entnehmen Sie die Diskette, und starten Sie den Computer neu. Der Computer startet mit dem USB Memory Key als Laufwerk C.

Die standardmäßige Boot-Reihenfolge variiert je nach Computer. Zudem kann Sie im Computer Setup (F10) Utility geändert werden.

Wenn Sie eine DOS-Version von Windows 9x verwendet haben, wird ggf. kurz ein Logo von Windows eingeblendet. Wenn diese Anzeige nicht eingeblendet werden soll, können Sie dem Stammverzeichnis des USB Memory Key eine Datei mit dem Namen LOGO.SYS und der Länge Null hinzufügen.

Fahren Sie mit „Kopieren auf mehrere Computer“ auf Seite 12 fort.

Nicht unterstützte USB-Flash-Media-Geräte

ACHTUNG: Nicht alle Computer können über ein USB-Flash-Media-Gerät gestartet werden. Wenn in der standardmäßigen Boot-Reihenfolge im Computer Setup (F10) Utility das USB-Gerät vor der Festplatte aufgelistet wird, kann der Computer über ein USB-Flash-Media-Gerät gestartet werden. Andernfalls muss eine bootfähige Diskette verwendet werden.

Für die Erstellung eines bootfähigen USB-Flash-Media-Geräts benötigen Sie Folgendes:

- Eines der folgenden Systeme:
  - Compaq Evo D510 Ultra-Slim Desktop
  - Compaq Evo D510 Convertible Minitower/Small Form Factor
  - HP Compaq Business Desktop D530 Serie – Ultra-Slim Desktop, Small Form Factor oder Convertible Minitower
  - Compaq Evo N400c, N410c, N600c, N610c, N620c, N800c oder N1000c Notebooks
  - Compaq Presario 1500 oder 2800 Notebooks

  Je nach BIOS unterstützen teilweise auch künftige Systeme Boot-Vorgänge über ein USB-Flash-Media-Gerät.

ACHTUNG: Wenn Sie einen anderen als die oben erwähnten Computer verwenden, sollten Sie sich vergewissern, dass in der standardmäßigen Boot-Reihenfolge im Computer Setup (F10) Utility das USB-Gerät vor der Festplatte genannt wird.

- Eine bootfähige DOS-Diskette mit den Programmen FDISK und SYS. Wenn SYS nicht verfügbar ist, kann auch FORMAT verwendet werden. Es gehen jedoch alle vorhandenen Dateien auf dem USB Memory Key verloren.

1. Wenn das System PCI-Karten enthält, an die SCSI-, ATA RAID-oder SATA-Laufwerke angeschlossen sind, müssen Sie den Computer ausschalten und den Netzstecker ziehen.

ACHTUNG: Das Netzkabel MUSS von der Stromversorgung getrennt werden.

2. Öffnen Sie den Computer, und entfernen Sie die PCI-Karten.
3. Schließen Sie das USB-Flash-Media-Gerät an einen der USB-Anschlüsse des Computers an, und entfernen Sie alle anderen USB-Speichergeräte außer den USB- Diskettenlaufwerken. Schließen Sie die Gehäuseabdeckung.
4. Stecken Sie den Netzstecker in eine Steckdose, und schalten Sie den Computer ein. Drücken Sie die Taste **F10**, sobald die LED-Anzeige am Monitor grün leuchtet, um das Setup-Dienstprogramm des Computers aufzurufen.
5. Zeigen Sie **Advanced/PCI devices** (Erweitert/PCI-Geräte) an, um sowohl die IDE- als auch die SATA-Controller zu deaktivieren. Achten Sie beim Deaktivieren des SATA-Controller auf den IRQ, dem der Controller zugewiesen ist. Sie müssen den IRQ später neu zuweisen. Beenden Sie das Setup, und bestätigen Sie die Änderungen

   SATA IRQ: _____
6. Legen Sie eine bootfähige DOS-Diskette mit FDISK.COM und SYS.COM oder FORMAT.COM in ein Diskettenlaufwerk ein, und schalten Sie den Computer ein, um diesen über die DOS-Diskette zu starten.
7. Führen Sie FDISK aus, und löschen Sie alle vorhandenen Partitionen auf dem USB-Flash-Media-Gerät. Erstellen Sie eine neue Partition, und aktivieren Sie diese. Beenden Sie FDISK, indem Sie die Taste **Esc** drücken.
8. Wenn das System nach dem Beenden von FDISK keinen automatischen Neustart durchführt, können Sie über die Tastenkombination **Strg+Alt+Entf** den Computer über die DOS-Diskette neu starten.
9. Geben Sie an der Eingabeaufforderung A:\ **FORMAT C: /S** ein, und drücken Sie die **Eingabetaste**. Der Befehl FORMAT formatiert das USB-Flash-Media-Gerät, fügt die Systemdateien hinzu und fordert eine Datenträgerbezeichnung an.
10. Drücken Sie die **Eingabetaste**, um keine Bezeichnung anzugeben, oder geben Sie einen Namen ein.
11. Schalten Sie den Computer aus, und ziehen Sie das Netzkabel. Öffnen Sie den Computer, und installieren Sie alle zuvor entnommenen PCI-Karten. Schließen Sie die Gehäuseabdeckung.

12. Stecken Sie den Netzstecker in eine Steckdose, entnehmen Sie die Diskette, und schalten Sie den Computer ein.
13. Drücken Sie die Taste **F10**, sobald die LED-Anzeige am Monitor grün leuchtet, um das Setup-Dienstprogramm des Computers aufzurufen.
14. Zeigen Sie **Advanced/PCI Devices** (Erweitert/PCI-Geräte) an, und aktivieren Sie die IDE- und SATA-Controller, die Sie in Schritt 5 deaktiviert haben. Platzieren Sie den SATA-Controller auf dem ursprünglichen IRQ.
15. Speichern Sie die Änderungen, und beenden Sie das Setup. Der Computer startet mit dem USB-Flash-Media-Gerät als Laufwerk C.

Die standardmäßige Boot-Reihenfolge variiert je nach Computer. Zudem kann Sie im Computer Setup (F10) Utility geändert werden.

Wenn Sie eine DOS-Version von Windows 9x verwendet haben, wird ggf. kurz ein Logo von Windows eingeblendet. Wenn diese Anzeige nicht eingeblendet werden soll, können Sie dem Stammverzeichnis des USB Memory Key eine Datei mit dem Namen LOGO.SYS und der Länge Null hinzufügen.

Fahren Sie mit „Kopieren auf mehrere Computer“ auf Seite 12 fort.

Dual-State-Netzschalter

Bei aktivierter ACPI-Funktion (Advanced Configuration and Power Interface) unter Windows 2000 und Windows XP Professional sowie Home Edition übernimmt der Netzschalter entweder die Funktion des Ein-/Aus-Schalters oder der Standby-Taste. Im Standby-Modus wird die Stromzufuhr nicht komplett unterbrochen, sondern der Computer schaltet auf geringen Stromverbrauch um. Dadurch können Sie schnell in den Energiesparmodus schalten, ohne die Anwendungen schließen zu müssen, und Sie können ohne Datenverlust schnell in den gleichen Betriebszustand zurückkehren.

So ändern Sie die Konfiguration des Netzschalters:

1. Klicken Sie unter Windows 2000 mit der linken Maustaste auf die Schaltfläche **Start**, und wählen Sie **Einstellungen > Systemsteuerung > Energieoptionen**.

   Klicken Sie unter Windows XP Professional und Home Edition mit der linken Maustaste auf die Schaltfläche **Start** und wählen Sie **Systemsteuerung > Leistung und Wartung > Energieoptionen** aus.

2. Öffnen Sie unter **Eigenschaften von Energieoptionen** die Registerkarte **Erweitert**.
3. Wählen Sie im Abschnitt **Netzschaltervorgänge** die gewünschten Einstellungen für den Netzschalter aus.

Wenn Sie den Netzschalter als Standby-Taste konfiguriert haben, wird das System durch Drücken des Schalters auf sehr geringen Stromverbrauch (Standby-Modus) umgeschaltet. Wenn Sie erneut auf die Standby-Taste drücken, schalten Sie aus dem Standby-Modus auf Normalbetrieb um. Wenn Sie die Stromzufuhr ganz unterbrechen wollen, halten Sie den Netzschalter vier Sekunden lang gedrückt.

ACHTUNG: Schalten Sie den Computer nur über den Netzschalter aus, wenn das System nicht mehr reagiert. Fahren Sie den Computer ansonsten über die Optionen des Betriebssystems herunter, da ansonsten die Gefahr der Beschädigung oder des Verlusts von Daten auf der Festplatte besteht.

WWW-Site

Die HP Techniker testen die von HP und Drittanbietern entwickelte Software nach strengen Richtlinien und entwickeln auf das jeweilige Betriebssystem zugeschnittene Support-Software, um eine optimale Leistung, Kompatibilität und Zuverlässigkeit von HP Computern zu gewährleisten.

Wenn Sie ein neues oder überarbeitetes Betriebssystem auf Ihrem Computer installieren, ist es wichtig, dass Sie auch die für das jeweilige Betriebssystem entwickelte Support-Software installieren. Wenn Sie mit einer Version von Microsoft Windows arbeiten möchten, die sich von der auf dem Computer vorinstallierten Version unterscheidet, müssen die entsprechenden Gerätetreiber und Dienstprogramme installiert werden, um sicherzustellen, dass alle Funktionen unterstützt werden und einwandfrei arbeiten.

HP hat das Auffinden, den Zugriff, die Bewertung und die Installation der neuesten Support-Software erheblich vereinfacht. Sie können die Software unter http://www.hp.com/support herunterladen.

Die Website enthält die neuesten Gerätetreiber, Dienstprogramme und Flash-ROM-Images, die zur Ausführung des neuesten Microsoft Windows Betriebssystems auf dem HP Computer erforderlich sind.

Bausteine und Partner

HP Management Lösungen können in andere Systemverwaltungslösungen integriert werden. Unter anderem werden die folgenden Branchenstandards beachtet:

- Desktop Management Interface (DMI) 2.0
- Wake on LAN-Technologie
- ACPI
- SMBIOS
- PXE (Pre-boot Execution)-Unterstützung

Bestandsüberwachung und Sicherheit

Die auf dem Computer vorinstallierten Bestandsüberwachungsfunktionen stellen Ihnen wichtige Daten zur Bestandsüberwachung bereit, die über HP Insight Manager, HP Client Manager oder andere Systemverwaltungsanwendungen verwaltet werden können. Die nahtlose automatische Integration in diese Produkte ermöglicht Ihnen die Auswahl des Management-Tools, das für die Umgebung am besten geeignet ist, ohne die bisherigen Investitionen in entsprechende Tools in Frage zu stellen.

Darüber hinaus bietet HP mehrere Lösungen zur Steuerung des Zugriffs auf wichtige Komponenten und Daten an. Wenn ProtectTools Embedded Security installiert wurde, verhindert dies einen nicht autorisierten Zugang zu Daten und prüft die Systemintegrität. Zudem werden Fremdbenutzer, die auf das System zugreifen, authentifiziert. Sicherheitsfunktionen wie ProtectTools, der Smart Cover Sensor und das Smart Cover Lock, die für bestimmte Modelle verfügbar sind, schützen gegen unberechtigten Zugriff auf interne Komponenten des Computers. Durch die Deaktivierung von parallelen und seriellen Anschlüssen sowie USB-Anschlüssen oder durch die Deaktivierung der Bootfähigkeit von Wechsellaufwerken können Sie wertvolle Datenbestände schützen. Memory Change- und Smart Cover Sensor-Warnmeldungen können automatisch an die Systemverwaltungsprogramme weitergeleitet werden, um darauf aufmerksam zu machen, dass sich jemand unerlaubten Zugang zu den internen Komponenten des Computers verschafft.

Protect Tools, der Smart Cover Sensor und das Smart Cover Lock stehen als Zusatzoptionen für ausgewählte Systeme zur Verfügung.

Verwenden Sie die folgenden Dienstprogramme zur Verwaltung der Sicherheitseinstellungen auf HP Computern.

- Lokal, mit Hilfe von Computer Setup Utility. Weitere Informationen und Anleitungen zur Verwendung dieses Dienstprogramms finden Sie im *Computer Setup (F10) Utility Handbuch*, das im Lieferumfang des Computers enthalten ist.
- Remote, mit HP Client Manager oder System Software Manager. Diese Software ermöglicht den sicheren, einheitlichen Einsatz und die Steuerung von Sicherheitseinstellungen über ein einfaches Befehlszeilen-Dienstprogramm.

Die folgende Tabelle und die folgenden Abschnitte beziehen sich auf das lokale Management von Sicherheitsfunktionen des Computers über Computer Setup (F10) Utility.

Überblick über die Sicherheitsfunktionen

Funktion	Zweck	Einrichtung
Removable Media Boot Control (Start-Schutz bei Wechsellaufwerken)	Verhindert den Systemstart von einem Wechsellaufwerk aus. (Ist nur für bestimmte Laufwerke verfügbar.)	Im Menü von Computer Setup (F10) Utility.
Serial, Parallel, USB, or Infrared Interface Control (Steuerung von seriellen, parallelen, USB- oder Infrarotschnittstellen)	Verhindert die Datenübertragung über die serielle, parallele, USB- oder Infrarotschnittstelle.	Im Menü von Computer Setup (F10) Utility.
Power-On Password (Kennwort für den Systemstart)	Verhindert den Zugriff auf den Computer bis zur Eingabe des Kennworts. Dies kann sowohl für den ersten Start als auch für einen Neustart gelten.	Im Menü von Computer Setup (F10) Utility.

✎ Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Funktion	Zweck	Einrichtung
Setup Password (Setup-Kennwort)	Der Computer kann erst dann (über Computer Setup Utility) neu konfiguriert werden, wenn das Setup-Kennwort eingegeben wird.	Im Menü von Computer Setup (F10) Utility.
Embedded Security Device (Integriertes Sicherheitsmodul)	Verhindert mit Hilfe von Verschlüsselung und Kennwortschutz den nicht autorisierten Zugang zu Daten. Überprüft die Systemintegrität und verlangt Authentifizierung von Fremdbenutzern, die auf das System zuzugreifen versuchen.	Im Menü von Computer Setup (F10) Utility.
DriveLock	Verhindert unbefugten Zugriff auf die Daten auf MultiBay Festplatten. Diese Funktion ist nur bei einigen Modellen verfügbar.	Im Menü von Computer Setup (F10) Utility.

✎ Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Funktion	Zweck	Einrichtung
Smart Cover Sensor	Zeigt an, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Kann so eingestellt werden, dass das Setup-Kennwort für den Neustart des Computers angegeben werden muss, wenn die Gehäuseabdeckung oder die Seitenabdeckung entfernt wurde. Weitere Informationen finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation Library* CD. Diese Funktion ist nur bei einigen Modellen verfügbar.	Im Menü von Computer Setup (F10) Utility.
Master Boot Record Security (Master Boot Record-Sicherheit)	Kann unbeabsichtigte oder böswillige Änderungen am Master Boot Record der aktuellen bootfähigen Festplatte verhindern und stellt ein Mittel zur Wiederherstellung des letzten als gut befundenen MBRs dar.	Im Menü von Computer Setup (F10) Utility.
Memory Change Alerts (Warnmeldungen bei Speicheränderungen)	Erkennt, ob Speichermodule hinzugefügt, verschoben oder entfernt wurden und benachrichtigt den Benutzer sowie den Systemadministrator.	Informationen zur Aktivierung dieser Warnmeldungen finden Sie im Online-Handbuch *Intelligent Manageability*.

✎ Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Überblick über die Sicherheitsfunktionen *(Fortsetzung)*

Funktion	Zweck	Einrichtung
Eigentümerkennung	Zeigt beim Systemstart Informationen über den Eigentümer (geschützt durch das Setup-Kennwort) an, die vom Systemadministrator eingegeben wurden.	Im Menü von Computer Setup (F10) Utility.
Kabelschloss	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können. Kann auch dazu verwendet werden, den Computer an einem unbeweglichen Gegenstand zu befestigen, um ihn gegen Diebstahl zu sichern.	Bringen Sie ein Kabelschloss an, um den Computer an einem unbeweglichen Gegenstand zu befestigen.
Ringschloss	Verhindert den Zugriff auf das Innere des Computers, damit keine Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden können.	Bringen Sie ein Ringschloss an, um zu verhindern, dass ungewollte Änderungen an der Konfiguration vorgenommen oder Komponenten entfernt werden.

✎ Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Die Unterstützung von Sicherheitsfunktionen kann je nach Computer-Konfiguration unterschiedlich sein.

Kennwort-Schutz

Das Kennwort für den Systemstart verhindert eine unbefugte Verwendung des Computers, indem für den Zugriff auf Anwendungen oder Daten bei jedem Einschalten oder Neustart des Computers die Eingabe eines Kennworts verlangt wird. Das Setup-Kennwort verhindert insbesondere den unbefugten Zugriff auf Computer Setup und kann auch zur Übergehung des Kennworts für den Systemstart verwendet werden. Der Zugriff auf den Computer wird also gewährt, wenn bei der Eingabeaufforderung für das Kennwort für den Systemstart statt dessen das Setup-Kennwort eingegeben wird.

Ein Kennwort für das gesamte Netzwerk kann festgelegt werden, damit der Systemadministrator sich für Wartungsarbeiten bei allen Netzwerksystemen anmelden kann, ohne das Kennwort für den Systemstart zu kennen, selbst wenn dieses festgelegt wurde.

Einrichten eines Setup-Kennworts über Computer Setup

Wenn das System mit einem integrierten Sicherheitsmodul ausgestattet ist, erhalten Sie unter „Integrierte Sicherheitsfunktion“ auf Seite 33 weitere Informationen.

Wenn ein Setup-Kennwort über Computer Setup eingerichtet wird, können Sie den Computer nur dann über Computer Setup Utility (F10) neu konfigurieren, wenn Sie das Kennwort eingeben.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Setup Password** (Setup-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Einrichten eines Kennworts beim Systemstart über Computer Setup

Die Einrichtung eines Kennworts für den Systemstart über Computer Setup verhindert den unbefugten Zugriff auf den Computer, wenn kein Kennwort eingegeben wird. Bei der Festlegung eines Kennworts für den Systemstart zeigt Computer Setup im Sicherheitsmenü Kennwortoptionen an. Als Kennwortoptionen steht **Password Prompt on Warm Boot** (Aufforderung zur Eingabe des Kennworts beim Warmstart) zur Auswahl. Bei Aktivierung dieser Option muss das Kennwort auch bei jedem Neustart eingegeben werden.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Power-On Password** (Systemstart-Kennwort). Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Eingeben eines Kennworts für den Systemstart

So geben Sie ein Kennwort für den Systemstart ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten.**
2. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das aktuelle Kennwort ein, und drücken Sie die **Eingabetaste**.

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Eingeben eines Setup-Kennworts

Wenn das System mit einem integrierten Sicherheitsmodul ausgestattet ist, erhalten Sie unter „Integrierte Sicherheitsfunktion“ auf Seite 33 weitere Informationen.

Wenn für den Computer ein Setup-Kennwort eingerichtet wurde, werden Sie jedes Mal zur Eingabe dieses Kennworts aufgefordert, wenn Sie das Programm Computer Setup starten.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten.**
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wenn das Schlüsselsymbol auf dem Bildschirm angezeigt wird, geben Sie das Setup-Kennwort ein, und drücken Sie die **Eingabetaste**.

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

Wenn Sie das Kennwort falsch eingeben, erscheint ein durchgestrichenes Schlüsselsymbol. Versuchen Sie es noch einmal. Nach drei misslungenen Versuchen müssen Sie den Computer aus- und wieder einschalten, um fortfahren zu können.

Ändern des Kennworts für den Systemstart oder des Setup-Kennworts

Wenn das System mit einem integrierten Sicherheitsmodul ausgestattet ist, erhalten Sie unter „Integrierte Sicherheitsfunktion“ auf Seite 33 weitere Informationen.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie **Computer Setup**, um das Setup-Kennwort zu ändern.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort, einen Schrägstrich (/) oder ein anderes Begrenzungszeichen, das neue Kennwort, einen weiteren Schrägstrich (/) oder ein anderes Begrenzungszeichen und ein zweites Mal das neue Kennwort folgendermaßen ein: **aktuelles Kennwort/neues Kennwort/neues Kennwort**

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

3. Drücken Sie die **Eingabetaste**.

Das neue Kennwort gilt ab dem nächsten Start des Computers.

Weitere Informationen zu anderen Begrenzungszeichen erhalten Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“ auf Seite 32. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Löschen des Kennworts für den Systemstart oder des Setup-Kennworts

Wenn das System mit einem integrierten Sicherheitsmodul ausgestattet ist, erhalten Sie unter „Integrierte Sicherheitsfunktion“ auf Seite 33 weitere Informationen.

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**. Starten Sie das Programm **Computer Setup**, um das Setup-Kennwort zu löschen.
2. Wenn das Schlüsselsymbol angezeigt wird, geben Sie das aktuelle Kennwort und einen Schrägstrich (/) oder ein anderes Begrenzungszeichen ein (siehe unten):
   aktuelles Kennwort/
3. Drücken Sie die **Eingabetaste**.

Weitere Informationen zu anderen Begrenzungszeichen erhalten Sie unter „Begrenzungszeichen auf landesspezifischen Tastaturen“. Das Kennwort für den Systemstart und das Setup-Kennwort können auch unter Verwendung der Sicherheitsfunktionen in Computer Setup geändert werden.

Begrenzungszeichen auf landesspezifischen Tastaturen

Jede Tastatur wurde an die landesspezifischen sprachlichen Besonderheiten angepasst. Die Syntax und die Tasten, die Sie zum Ändern oder Löschen des Kennworts verwenden, hängen von der mit dem Computer gelieferten Tastatur ab.

Begrenzungszeichen auf landesspezifischen Tastaturen

Arabisch	/	Griechisch	-	Russisch	/
Belgisch	=	Hebräisch	.	Slowakisch	-
BHKSJ*	-	Ungarisch	-	Spanisch	-
Brasilianisch	/	Italienisch	-	Schwedisch/ Finnisch	/
Chinesisch	/	Japanisch	/	Schweizerisch	-
Tschechisch	-	Koreanisch	/	Taiwanesisch	/
Dänisch	-	Lateinamerikanisch (Spanisch/ Portugiesisch)	-	Thailändisch	/
Französisch	!	Norwegisch	-	Türkisch	.
Kan. Französisch	é	Polnisch	-	Britisches Englisch	/
Deutsch	-	Portugiesisch	-	Amerikanisches Englisch	/

* Bosnien-Herzegowina, Kroatien, Slowenien und Jugoslawien

Löschen von Kennwörtern

Wenn Sie das Kennwort nicht mehr wissen, können Sie nicht mehr auf den Computer zugreifen. Anleitungen zum Löschen von Kennwörtern finden Sie im *Fehlerbeseitigungs-Handbuch*.

Wenn das System mit einem integrierten Sicherheitsmodul ausgestattet ist, erhalten Sie unter „Integrierte Sicherheitsfunktion“ weitere Informationen.

Integrierte Sicherheitsfunktion

ProtectTools Embedded Security kombiniert Verschlüsselung und Kennwortschutz. Auf diese Weise wird ein erweiterter Schutz für EFS-Dateiverschlüsselungen /-Ordnerverschlüsselungen (Embedded File System) sowie für E-Mails in Microsoft Outlook und Outlook Express erzielt. ProtectTools ist für ausgewählte Business-Desktops als Option in individuell konfigurierten Systemen (Configured-To-Order, CTO) erhältlich. Es richtet sich an HP Kunden, deren oberste Priorität der Schutz der Daten ist, da der nicht autorisierte Datenzugang eine wesentlich größere Gefahr darstellt als ein Datenverlust. ProtectTools verwendet vier Kennwörter:

- (F10) Setup – Wird für den Zugriff auf das Computer Setup (F10) Utility und zum Aktivieren bzw. Deaktivieren von ProtectTools verwendet.
- Take Ownership (Besitz übernehmen) – Wird von einem Systemadministrator eingestellt und verwendet, der den Benutzern Rechte zuweist und Sicherheitsparameter einstellt.
- Emergency Recovery Token (Wiederherstellungs-Token) – Wird vom Systemadministrator eingestellt und ermöglicht die Wiederherstellung nach einem Ausfall des Computers oder des ProtectTools-Chips.
- Basic User (Standardbenutzer) – Wird vom Endbenutzer eingestellt und verwendet.

Wenn des Kennwort des Endbenutzers verloren geht, können die verschlüsselten Daten nicht wiederhergestellt werden. Deshalb ist die Verwendung von ProtectTools am sichersten, wenn die auf dem Laufwerk des Benutzers enthaltenen Daten in ein Systeminformationssystem repliziert oder regelmäßig gesichert werden.

ProtectTools Embedded Security ist ein Sicherheitschip entsprechend TCPA 1.1, der optional auf der Systemplatine von ausgewählten Business-Desktops installiert werden kann. Jeder ProtectTools Embedded Security-Chip ist einmalig und an einen spezifischen Computer gebunden. Der Chip führt grundlegende Sicherheitsprozesse unabhängig von anderen Computerkomponenten (z. B. Prozessor, Speicher oder Betriebssystem) durch.

Ein ProtectTools Embedded Security-fähiger Computer erweitert und verbessert die Sicherheitsfunktionen von Microsoft Windows 2000 oder Windows XP Professional bzw. Home Edition. Das Betriebssystem kann beispielsweise lokale Dateien und Ordner basierend auf EFS verschlüsseln, während ProtectTools Embedded Security mit der Erstellung von Schlüsseln anhand des Stammschlüssels der Plattform (der auf der Platine gespeichert ist) über eine weitere Sicherheitsebene verfügt. Dieser Prozess wird als „Wrapping“ bezeichnet. ProtectTools verhindert jedoch keinen Netzwerkzugang zu Computern ohne ProtectTools.

Hauptmerkmale von ProtectTools Embedded Security:

- Plattformauthentifizierung
- Speicherschutz
- Datenintegrität

ACHTUNG: Achten Sie darauf, dass Sie Ihre Kennwörter nicht vergessen. **Verschlüsselte Daten können ohne Kennwort weder gelesen noch wiederhergestellt werden**.

Festlegen von Kennwörtern

Setup

Es kann ein Setup-Kennwort erstellt werden, und das integrierte Sicherheitsmodul kann mit Hilfe des Setup Utility F10 aktiviert werden.

1. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

2. Wähle Sie mit den Nach-oben- und Nach-unten-Tasten eine Sprache aus, und drücken Sie die **Eingabetaste**.

3. Zeigen Sie mit Hilfe der Nach-rechts- und Nach-links-Tasten die Registerkarte **Security** (Sicherheit) an, und aktivieren Sie mit den Nach-oben- und Nach-unten-Tasten **Setup Password** (Setup-Kennwort). Drücken Sie die **Eingabetaste**.
4. Geben Sie ein Kennwort ein, und bestätigen Sie es. Drücken Sie die Taste **F10**, um das Kennwort zu übernehmen.

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

5. Aktivieren Sie mit Hilfe der Nach-oben- und Nach-unten-Tasten **Embedded Security Device** (Integriertes Sicherheitsmodul). Drücken Sie die **Eingabetaste**.
6. Wenn im Dialogfeld **Embedded Security Device – Disable** (Integrierte Sicherheitsfunktion – Deaktivieren) aktiviert ist, können Sie die Einstellung über die Nach-links- und Nach-rechts-Taste in **Embedded Security Device – Enable** (Integriertes Sicherheitsmodul – Aktivieren) ändern. Drücken Sie die Taste **F10**, um die Änderung zu übernehmen.

ACHTUNG: Wenn Sie **Reset to Factory Settings – Reset** (Auf Voreinstellungen zurücksetzen – Zurücksetzen) auswählen, werden alle Schlüssel gelöscht. Verschlüsselte Daten können in diesem Fall *nur* wiederhergestellt werden, wenn die Schlüssel gesichert wurden (siehe „Take Ownership (Besitz übernehmen) und Emergency Recovery Token (Wiederherstellungs-Token)“). Wählen Sie **Reset** (Zurücksetzen) daher nur aus, wenn Sie in der Anleitung zur Wiederherstellung verschlüsselter Daten eine eindeutige Anleitung erhalten haben (siehe „Wiederherstellen verschlüsselter Daten“ auf Seite 38).

7. Aktivieren Sie mit Hilfe der Nach-links- und Nach-rechts-Taste **File** (Datei). Aktivieren Sie mit Hilfe der Nach-oben- und Nach-unten-Tasten **Save Changes and Exit** (Änderungen speichern und Beenden). Drücken Sie die **Eingabetaste**, und anschließend zur Bestätigung die Taste **F10**.

Take Ownership (Besitz übernehmen) und Emergency Recovery Token (Wiederherstellungs-Token)

Das Take Ownership-Kennwort wird zum Aktivieren und Deaktivieren der Sicherheitsplattform sowie zum Autorisieren von Benutzern benötigt. Wenn das integrierte Sicherheitsmodul ausfällt, ermöglicht der Wiederherstellungsfunktion die Benutzerautorisierung und den Datenzugang.

1. Klicken Sie bei Verwendung von Windows XP Professional oder Home Edition auf **Start > Alle Programme > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

   Klicken Sie bei Verwendung von Windows 2000 auf **Start > Programme > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

2. Klicken Sie auf **Next** (Weiter).
3. Geben Sie das Take Ownership-Kennwort ein, und bestätigen Sie es. Klicken Sie anschließend auf **Next** (Weiter).

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Klicken Sie auf **Next** (Weiter), um das Standardverzeichnis für die Wiederherstellung zu übernehmen.
5. Geben Sie das Kennwort für das Wiederherstellungs-Token ein, und bestätigen Sie es. Klicken Sie anschließend auf **Next** (Weiter).
6. Legen Sie eine Diskette ein, auf der der Schlüssel für das Wiederherstellungs-Token gespeichert werden soll. Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie die Diskette aus.

ACHTUNG: Dieser Schlüssel wird zur Wiederherstellung verschlüsselter Daten verwendet, wenn der Computer oder ein integrierter Sicherheitschip ausfallen. **Die Daten können ohne den Schlüssel nicht wiederhergestellt werden**. (Zudem benötigen Sie für den Zugriff auf die Daten das Basic User-Kennwort.) Lagern Sie die Diskette an einem sicheren Ort.

7. Klicken Sie auf **Save** (Speichern), um das Verzeichnis und den standardmäßigen Dateinamen zu übernehmen, und klicken Sie anschließend auf **Next** (Weiter).
8. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen, bevor die Sicherheitsplattform initialisiert wird.

Es wird ggf. eine Meldung angezeigt, derzufolge die integrierten Sicherheitsfunktionen nicht initialisiert sind. Klicken Sie nicht auf die Meldung. Die Initialisierung erfolgt im weiteren Verlauf des Verfahrens, und die Meldung wird nach wenigen Sekunden automatisch ausgeblendet.

9. Klicken Sie auf **Next** (Weiter), um die Konfiguration der lokalen Richtlinien zu überspringen.
10. Vergewissern Sie sich, dass das Kontrollkästchen **Start Embedded Security User Initialization Wizard** aktiviert ist, und klicken Sie anschließend auf **Finish** (Fertig stellen).

Der User Initialization Wizard wird nun automatisch gestartet.

Basic User (Standardbenutzer)

Während der Benutzerinitialisierung wird das Basic User-Kennwort erstellt. Dieses Kennwort wird für die Eingabe und den Zugriff auf verschlüsselte Daten benötigt.

ACHTUNG: Achten Sie darauf, dass Sie Ihr Basic User-Kennwort nicht vergessen. **Verschlüsselte Daten können ohne dieses Kennwort weder gelesen noch wiederhergestellt werden**.

1. Gehen Sie folgendermaßen vor, wenn der User Initialization Wizard nicht geöffnet ist:

   Klicken Sie bei Verwendung von Windows XP Professional oder Home Edition auf **Start > Alle Programme > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

   Klicken Sie bei Verwendung von Windows 2000 auf **Start > Programme > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
2. Klicken Sie auf **Next** (Weiter).

3. Geben Sie das Kennwort für den Standardbenutzer-Schlüssel ein, und bestätigen Sie es. Klicken Sie anschließend auf **Next** (Weiter).

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

4. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
5. Wählen Sie geeignete Sicherheitsfunktionen aus, und klicken Sie auf **Next** (Weiter).
6. Wählen Sie den geeigneten E-Mail-Client aus, und klicken Sie auf **Next** (Weiter).
7. Klicken Sie auf **Next** (Weiter), um das Verschlüsselungszertifikat anzuwenden.
8. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
9. Klicken Sie auf **Finish** (Fertig stellen).
10. Starten Sie den Computer neu.

Wiederherstellen verschlüsselter Daten

Für die Wiederherstellung von Daten nach einem Austausch des ProtectTools-Chips benötigen Sie Folgendes:

- SPEmRecToken.xml – Schlüssel für das Wiederherstellungs-Token
- SPEmRecArchive.xml – Verborgener Ordner. Standardverzeichnis: C:\Dokumente und Einstellungen\All Users\Application Data\Infineon\TPM Software\Recovery Archive
- ProtectTools-Kennwörter
  - Setup
  - Take Ownership (Besitz übernehmen)
  - Emergency Recovery Token (Wiederherstellungs-Token)
  - Basic User (Standardbenutzer)

1. Starten Sie den Computer neu.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Geben Sie das Setup-Kennwort ein, und drücken Sie die **Eingabetaste**.
4. Wählen Sie mit den Nach-oben- und Nach-unten-Tasten eine Sprache aus, und drücken Sie die **Eingabetaste**.
5. Zeigen Sie mit Hilfe der Nach-rechts- und Nach-links-Tasten die Registerkarte **Security** (Sicherheit) an, und aktivieren Sie mit den Nach-oben- und Nach-unten-Tasten **Embedded Security Device** (Integriertes Sicherheitsmodul). Drücken Sie die **Eingabetaste**.
6. Gehen Sie wie folgt vor, wenn nur die Option **Embedded Security Device – Disable** (Integriertes Sicherheitsmodul – Deaktivieren) verfügbar ist:

   a. Aktivieren Sie mit Hilfe der Nach-links- und Nach-rechts-Tasten **Embedded Security Device – Enable** (Integriertes Sicherheitsmodul – Aktivieren). Drücken Sie die Taste **F10**, um die Änderung zu übernehmen.

   b. Aktivieren Sie mit Hilfe der Nach-links- und Nach-rechts-Taste **File** (Datei). Aktivieren Sie mit Hilfe der Nach-oben- und Nach-unten-Tasten **Save Changes and Exit** (Änderungen speichern und Beenden). Drücken Sie die **Eingabetaste**, und anschließend zur Bestätigung die Taste **F10**.

   c. Fahren Sie mit Schritt 1 fort.

   Wenn zwei Optionen verfügbar sind, fahren Sie mit Schritt 7 fort.
7. Aktivieren Sie mit den Nach-oben- und Nach-unten-Tasten **Reset to Factory Settings – Do Not Reset** (Auf Voreinstellungen zurücksetzen – Nicht zurücksetzen). Drücken Sie einmal die Nach-links- oder Nach-rechts-Taste.

   Es wird eine Meldung mit etwa folgendem Text angezeigt: Durch diesen Vorgang wird das integrierte Sicherheitsmodul auf die Voreinstellungen zurückgesetzt, wenn die Einstellungen beim Beenden gespeichert werden. Drücken Sie zum Fortfahren eine beliebige Taste.

   Drücken Sie die **Eingabetaste**.
8. Die ausgewählte Option lautet nun **Reset to Factory Settings – Reset** (Auf Voreinstellungen zurücksetzen – Zurücksetzen). Drücken Sie die Taste **F10**, um die Änderung zu übernehmen.

9. Aktivieren Sie mit Hilfe der Nach-links- und Nach-rechts-Taste **File** (Datei). Aktivieren Sie mit Hilfe der Nach-oben- und Nach-unten-Tasten **Save Changes and Exit** (Änderungen speichern und Beenden). Drücken Sie die **Eingabetaste**, und anschließend zur Bestätigung die Taste **F10**.
10. Starten Sie den Computer neu.
11. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

12. Geben Sie das Setup-Kennwort ein, und drücken Sie die **Eingabetaste**.
13. Wählen Sie mit den Nach-oben- und Nach-unten-Tasten eine Sprache aus, und drücken Sie die **Eingabetaste**.
14. Zeigen Sie mit Hilfe der Nach-rechts- und Nach-links-Tasten die Registerkarte **Security** (Sicherheit) an, und aktivieren Sie mit den Nach-oben- und Nach-unten-Tasten **Embedded Security Device** (Integriertes Sicherheitsmodul). Drücken Sie die **Eingabetaste**.
15. Wenn im Dialogfeld **Embedded Security Device – Disable** (Integriertes Sicherheitsmodul – Deaktivieren) aktiviert ist, können Sie die Einstellung über die Nach-links- und Nach-rechts-Taste in **Embedded Security Device – Enable** (Integriertes Sicherheitsmodul – Aktivieren) ändern. Drücken Sie die Taste **F10**.
16. Aktivieren Sie mit Hilfe der Nach-links- und Nach-rechts-Taste **File** (Datei). Aktivieren Sie mit Hilfe der Nach-oben- und Nach-unten-Tasten **Save Changes and Exit** (Änderungen speichern und Beenden). Drücken Sie die **Eingabetaste**, und anschließend zur Bestätigung die Taste **F10**.

17. Gehen Sie nach dem Öffnen von Windows wie folgt vor:

    Klicken Sie bei Verwendung von Windows XP Professional oder Home Edition auf **Start > Alle Programme > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

    Klicken Sie bei Verwendung von Windows 2000 auf **Start > Programme > HP ProtectTools Embedded Security Tools > Embedded Security Initialization Wizard**.

18. Klicken Sie auf **Next** (Weiter).
19. Geben Sie ein Take Ownership-Kennwort ein, und bestätigen Sie es. Klicken Sie auf **Next** (Weiter).

Nehmen Sie die Eingabe sorgfältig vor. Aus Sicherheitsgründen werden die eingegebenen Zeichen auf dem Bildschirm nicht angezeigt.

20. Vergewissern Sie sich, dass die Erstellung eines neuen Wiederherstellungsarchivs aktiviert ist. Klicken Sie unter **Recovery archive location** (Verzeichnis für Wiederherstellungsarchiv) auf **Browse** (Durchsuchen).
21. Übernehmen Sie nicht den standardmäßigen Dateinamen. Geben Sie einen neuen Dateinamen ein, so dass die Originaldatei nicht überschrieben wird.
22. Klicken Sie auf **Save** (Speichern) und anschließend auf **Next** (Weiter).
23. Geben Sie das Kennwort für das Wiederherstellungs-Token ein, und bestätigen Sie es. Klicken Sie anschließend auf **Next** (Weiter).
24. Legen Sie eine Diskette ein, auf der der Schlüssel für das Wiederherstellungs-Token gespeichert werden soll. Klicken Sie auf **Browse** (Durchsuchen), und wählen Sie die Diskette aus.
25. Übernehmen Sie nicht den standardmäßigen Schlüsselnamen. Geben Sie einen neuen Schlüsselnamen ein, so dass der Originalschlüssel nicht überschrieben wird.
26. Klicken Sie auf **Save** (Speichern) und anschließend auf **Next** (Weiter).

27. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen, bevor die Sicherheitsplattform initialisiert wird.

Es wird ggf. eine Meldung angezeigt, derzufolge der Standardbenutzer-Schlüssel nicht geladen werden kann. Klicken Sie nicht auf die Meldung. Die Initialisierung erfolgt im weiteren Verlauf des Verfahrens, und die Meldung wird nach wenigen Sekunden automatisch ausgeblendet.

28. Klicken Sie auf **Next** (Weiter), um die Konfiguration der lokalen Richtlinien zu überspringen.
29. Deaktivieren Sie das Kontrollkästchen **Start Embedded Security User Initialization Wizard** (Embedded Security User Initialization Wizard starten). Klicken Sie auf **Finish** (Fertig stellen).
30. Klicken Sie in der Symbolleiste mit der rechten Maustaste auf das Symbol von ProtectTools, und wählen Sie **Initialize Embedded Security restoration** (Wiederherstellung der integrierten Sicherheit initialisieren) aus.

    Auf diese Weise wird der HP ProtectTools Embedded Security Initialization Wizard gestartet.
31. Klicken Sie auf **Next** (Weiter).
32. Legen Sie die Diskette ein, auf der der ursprüngliche Schlüssel für das Wiederherstellungs-Token gespeichert ist. Klicken Sie auf **Browse** (Durchsuchen), suchen Sie das Token, und doppelklicken Sie auf dieses, um den Namen in das Feld einzugeben. Der Standardname ist „A:\SPEmRecToken.xml“.
33. Geben Sie das Originalkennwort des Tokens ein, und klicken Sie auf **Next** (Weiter).
34. Klicken Sie auf **Browse** (Durchsuchen), suchen Sie das ursprüngliche Wiederherstellungsarchiv, und doppelklicken Sie auf dieses, um den Namen in das Feld einzugeben. Der Standardname ist „C:\Dokumente und Einstellungen\All Users\Application Data\Infineon\TPM Software\RecoveryArchive\SPEmRecArchive.xml“.
35. Klicken Sie auf **Next** (Weiter).

36. Klicken Sie auf den Computer, der wiederhergestellt werden soll, und anschließend auf **Next** (Weiter).
37. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
38. Wenn der Assistent angibt, dass die Sicherheitsplattform wiederhergestellt wurde, fahren Sie mit Schritt 39 fort.

    Wenn der Assistent angibt, dass die Wiederherstellung fehl geschlagen ist, fahren Sie mit Schritt 10 fort. Überprüfen Sie sorgfältig die Kennwörter, das Token-Verzeichnis und den Token-Namen sowie das Archivverzeichnis und den Archivnamen.
39. Klicken Sie auf **Finish** (Fertig stellen).
40. Klicken Sie bei Verwendung von Windows XP Professional oder Home Edition auf **Start > Alle Programme > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.

    Klicken Sie bei Verwendung von Windows 2000 auf **Start > Programme > HP ProtectTools Embedded Security Tools > User Initialization Wizard**.
41. Klicken Sie auf **Next** (Weiter).
42. Klicken Sie auf **Recover your basic user key** (Standardbenutzer-Schlüssel wiederherstellen) und anschließend auf **Next** (Weiter).
43. Wählen Sie einen Benutzer aus, geben Sie das ursprüngliche Kennwort für den Standardbenutzer-Schlüssel für diesen Benutzer ein, und klicken Sie anschließend auf **Next** (Weiter).
44. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen und das Standardverzeichnis für die Wiederherstellung zu übernehmen.

Durch die Schritte 45 bis 49 wird die Basic User-Originalkonfiguration erneut installiert.

45. Wählen Sie geeignete Sicherheitsfunktionen aus, und klicken Sie auf **Next** (Weiter).
46. Wählen Sie den geeigneten E-Mail-Client aus, und klicken Sie auf **Next** (Weiter).

47. Klicken Sie auf das Verschlüsselungszertifikat und anschließend auf **Next** (Weiter), um dieses anzuwenden.
48. Klicken Sie auf **Next** (Weiter), um die Einstellungen zu bestätigen.
49. Klicken Sie auf **Finish** (Fertig stellen).
50. Starten Sie den Computer neu.

ACHTUNG: Achten Sie darauf, dass Sie Ihr Basic User-Kennwort nicht vergessen. **Verschlüsselte Daten können ohne dieses Kennwort weder gelesen noch wiederhergestellt werden**.

DriveLock

DriveLock ist eine Sicherheitsfunktion, die den unbefugten Zugriff auf Daten auf MultiBay Festplatten verhindert. DriveLock wurde als Erweiterung von Computer Setup entwickelt. Es ist jedoch nur verfügbar, wenn eine DriveLock-fähige Festplatte vorhanden ist.

DriveLock richtet sich an HP Kunden, deren oberste Priorität der Schutz der Daten ist. Für diese Kunden stehen die Kosten einer Festplatte und der Verlust der darauf gespeicherten Daten in keinem Verhältnis zu dem Schaden, der bei unberechtigtem Zugriff auf ihren Inhalt entstehen kann. Damit dieses hohe Sicherheitsniveau nicht zu allzu großen Problemen führt, wenn ein Kennwort vergessen wird, verwendet die HP Implementierung von DriveLock ein Sicherheitssystem mit zwei Kennwörtern. Dabei sollte ein Kennwort vom Systemadministrator festgelegt und verwendet werden, während das zweite normalerweise vom Benutzer erstellt und verwendet wird. Wenn beide Kennwörter vergessen werden, gibt es keine Möglichkeit mehr, die Laufwerksperre aufzuheben. Deshalb ist die Verwendung von DriveLock am sichersten, wenn die auf der Festplatte enthaltenen Daten in ein Firmeninformationssystem repliziert oder regelmäßig gesichert werden.

Falls beide Kennwörter für DriveLock vergessen werden, bleibt der Zugriff auf die Festplatte für immer gesperrt. Dies stellt für Benutzer, die nicht dem obigen Kundenprofil entsprechen, unter Umständen ein inakzeptables Risiko dar. Für Benutzer jedoch, die dem Profil entsprechen, bedeutet es im Hinblick auf die auf der Festplatte gespeicherten Daten ein Risiko, das hingenommen werden kann.

Verwenden von DriveLock

In Computer Setup ist DriveLock eine Option im Sicherheitsmenü. Dem Benutzer stehen Möglichkeiten zur Festlegung des Masterkennworts oder zur Aktivierung von DriveLock zur Verfügung. Zur Aktivierung von DriveLock muss ein Benutzerkennwort angegeben werden. Da die erste Konfiguration von DriveLock normalerweise vom Systemadministrator ausgeführt wird, sollte zuerst ein Masterkennwort festgelegt werden. HP befürwortet immer die Festlegung eines Masterkennworts durch den Administrator, unabhängig davon, ob DriveLock aktiviert werden soll. Dadurch hat der Administrator die Möglichkeit, DriveLock-Einstellungen zu ändern, wenn das Laufwerk einmal gesperrt sein sollte. Ist das Masterkennwort festgelegt, kann der Administrator DriveLock entweder aktivieren oder deaktiviert lassen.

Bei einer gesperrten Festplatte wird beim POST ein Kennwort zum Aufheben der Sperre abgefragt. Wenn ein Kennwort für den Systemstart festgelegt ist, das dem Benutzerkennwort für das Gerät entspricht, wird beim POST nicht erneut zur Eingabe des Kennworts aufgefordert. Andernfalls wird der Benutzer zur Eingabe eines DriveLock-Kennworts aufgefordert. Dabei kann entweder das Master- oder das Benutzerkennwort verwendet werden. Benutzern stehen zwei Versuche zur richtigen Kennworteingabe frei. Wird zweimal das falsche Kennwort eingegeben, wird der POST fortgesetzt, es besteht aber kein Zugriff auf Daten der Festplatte.

Anwendungen von DriveLock

Am besten ist die DriveLock-Sicherheitsfunktion für eine Firmenumgebung geeignet, in der die Computer einiger Benutzer mit MultiBay Festplatten ausgestattet sind. Der Systemadministrator hat die Aufgabe, das MultiBay Festplattenlaufwerk zu konfigurieren, das heißt unter anderem, auch das DriveLock-Masterkennwort festzulegen. Falls der Benutzer das Benutzerkennwort vergisst oder das Gerät an einen anderen Mitarbeiter weitergegeben wird, kann das Masterkennwort immer dazu verwendet werden, das Benutzerkennwort zurückzusetzen oder auf die Festplatte zuzugreifen.

HP empfiehlt Systemadministratoren, die DriveLock aktivieren möchten, die Erstellung einer Firmenrichtlinie zur Einrichtung und Verwaltung von Masterkennwörtern. Dadurch soll vermieden werden, dass ein Mitarbeiter vor seinem Ausscheiden aus der Firma absichtlich oder unabsichtlich beide DriveLock-Kennwörter festlegt. In einem solchen Fall würde die Festplatte unbrauchbar und müsste ersetzt werden. Außerdem könnte es passieren, dass Systemadministratoren, die kein Masterkennwort festlegen, selbst eine gesperrte Festplatte vorfinden und dadurch keine Routineüberprüfungen auf nicht autorisierte Software, andere Bestandskontrollfunktionen und Supportaktivitäten mehr ausführen können.

Benutzern mit niedrigeren Sicherheitsanforderungen empfiehlt HP die Aktivierung von DriveLock nicht. Dazu zählen private Benutzer oder Benutzer, die auf ihrer Festplatte im Normalfall keine streng geheimen Daten aufbewahren. Für diese Benutzer ist der mögliche Verlust einer Festplatte aufgrund von zwei vergessenen Kennwörtern größer als der Wert, der mit DriveLock geschützt wird. Der Zugriff auf Computer Setup und DriveLock kann durch das Setup-Kennwort eingeschränkt werden. Durch das Festlegen eines Setup-Kennworts, das nicht an Endbenutzer weitergegeben wird, können Systemadministratoren vermeiden, dass Benutzer DriveLock aktivieren.

Smart Cover Sensor

Der Smart Cover Sensor (nur bei einigen Modellen), eine Kombination aus Hardware- und Softwaretechnologie, gibt eine Warnmeldung aus, wenn die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Es gibt drei Schutzstufen, die in der folgenden Tabelle beschrieben werden.

Schutzstufen des Smart Cover Sensors

Stufe	Einstellung	Beschreibung
Stufe 0	Disabled (Deaktiviert)	Der Smart Cover Sensor ist deaktiviert (Standardeinstellung).
Stufe 1	Notify User (Benutzer benachrichtigen)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde.
Stufe 2	Setup Password (Setup-Kennwort)	Wenn der Computer neu gestartet wird, wird auf dem Bildschirm eine Meldung darüber angezeigt, dass die Gehäuseabdeckung bzw. die Seitenabdeckung entfernt wurde. Sie müssen das Setup-Kennwort eingeben, um fortfahren zu können.

✎ Diese Einstellungen können mit Hilfe von Computer Setup geändert werden. Weitere Informationen zu Computer Setup finden Sie im *Computer Setup (F10) Utility Handbuch*.

Einstellen der Schutzstufe für den Smart Cover Sensor

So stellen Sie eine Schutzstufe für den Smart Cover Sensor ein:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security** (Sicherheit) und anschließend **Smart Cover**. Folgen Sie dann den Anleitungen auf dem Bildschirm.
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Smart Cover Lock

Das Smart Cover Lock ist eine über die Software gesteuerte Abdeckungsverriegelung, mit der einige HP Computer ausgestattet sind. Diese Funktion verhindert den unbefugten Zugriff auf die inneren Komponenten des Computers. Die Computer werden mit deaktiviertem Smart Cover Lock geliefert.

ACHTUNG: Für die maximale Sicherheit der Abdeckungsverriegelung müssen Sie ein Setup-Kennwort einrichten. Das Setup-Kennwort verhindert den unbefugten Zugriff auf Computer Setup.

Das Smart Cover Lock ist als Zusatzoption für bestimmte Systeme erhältlich.

Aktivieren des Smart Cover Lock

So aktivieren Sie die Sperrfunktion des Smart Cover Lock:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security** (Sicherheit), dann **Smart Cover** und anschließend die Option **Locked** (Gesperrt).
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Aufheben der Sperre des Smart Cover Lock

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security > Smart Cover > Unlocked** (Sicherheit > Smart Cover > Sperre aufgehoben).
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Verwenden des Smart Cover FailSafe-Schlüssels

Wenn das Smart Cover Lock aktiviert ist und Sie das Benutzerkennwort nicht eingeben können, um die Sperre zu deaktivieren, brauchen Sie einen Smart Cover FailSafe-Schlüssel, um die Gehäuseabdeckung öffnen zu können. Der Schlüssel ist in den folgenden Fällen erforderlich:

- Stromausfall
- Fehlgeschlagener Systemstart
- Ausfall einer PC-Komponente (z. B. Prozessor oder Netzteil)
- Kennwort vergessen

ACHTUNG: Der Smart Cover FailSafe-Schlüssel ist ein spezielles Werkzeug, das von HP angeboten wird. Vermeiden Sie lange Ausfallzeiten bei unliebsamen Überraschungen, und bestellen Sie den Schlüssel bei einem Servicepartner.

Führen Sie eines der folgenden Verfahren durch, um den FailSafe-Schlüssel zu erhalten:

- Wenden Sie sich an einen HP Servicepartner.
- Rufen Sie die in der Garantieerklärung genannte Nummer an.

Weitere Informationen zur Verwendung des Smart Cover FailSafe-Schlüssels finden Sie im *Hardware-Referenzhandbuch*.

Master Boot Record Security (Master Boot Record-Sicherheit)

Der Master Boot Record (MBR) enthält Informationen, die für den erfolgreichen Start von einer Diskette aus und den Zugriff auf die auf der Diskette gespeicherten Daten erforderlich sind. Mit Hilfe von Master Boot Record Security können unbeabsichtigte oder böswillige Änderungen am MBR verhindert werden, die beispielsweise durch Viren oder die unkorrekte Verwendung von bestimmten Festplatten-dienstprogrammen verursacht werden. Sie haben außerdem die Möglichkeit, den letzten als gut befundenen MBR wiederherzustellen, wenn Sie beim Neustart des Systems Änderungen am MBR feststellen.

So aktivieren Sie die MBR-Sicherheit:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security > Master Boot Record Security > Enabled.** (Sicherheit > Master Boot Record-Sicherheit > Aktiviert).
4. Wählen Sie **Security > Save Master Boot Record** (Sicherheit > Master Boot Record speichern).
5. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Wenn die MBR-Sicherheit aktiviert ist, verhindert das BIOS sämtliche Änderungen am MBR der aktuellen bootfähigen Festplatte, solange in MS-DOS oder Windows der geschützte Modus aktiviert ist.

Die meisten Betriebssysteme steuern den Zugriff auf den MBR der aktuellen bootfähigen Festplatte. Das BIOS kann keine Änderungen verhindern, die während der Ausführung des Betriebssystems erfolgen.

Bei jedem Einschalten oder Neustart des Computers vergleicht das BIOS den MBR der aktuellen bootfähigen Festplatte mit dem zuvor gespeicherten MBR. Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen bootfähigen Festplatte um dieselbe Festplatte handelt, von welcher der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

1999 – Master Boot Record has changed (1999 – Master Boot Record wurde geändert).

Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte
- Wiederherstellen des zuvor gespeicherten MBR oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

Wenn Änderungen festgestellt werden und wenn es sich bei der aktuellen bootfähigen Festplatte **nicht** um dieselbe Festplatte handelt, von der der MBR zuvor gespeichert wurde, wird die folgende Meldung angezeigt:

2000 – Master Boot Record Hard Drive has changed (Master Boot Record der Festplatte wurde geändert).

Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

In dem unwahrscheinlichen Fall, dass der zuvor gespeicherte MBR beschädigt wurde, wird die folgende Meldung angezeigt:

1998 – Master Boot Record has been lost (1998 – Master Boot Record ist verloren gegangen).

Drücken Sie eine beliebige Taste, um Computer Setup zu starten und die MBR-Sicherheit zu konfigurieren.

Wenn Sie Computer Setup starten, müssen Sie die folgenden Aktionen durchführen:

- Speichern des MBR der aktuellen bootfähigen Festplatte oder
- Deaktivieren der MBR-Sicherheitsfunktion.

Sie benötigen das Setup-Kennwort, falls ein Kennwort eingerichtet wurde.

Maßnahmen vor der Partitionierung oder Formatierung der aktuellen bootfähigen Festplatte

Stellen Sie sicher, dass die MBR-Sicherheit deaktiviert ist, bevor Sie die Formatierung oder Partitionierung der aktuellen bootfähigen Festplatte ändern. Einige Festplattendienstprogramme (wie z. B. FDISK und FORMAT) versuchen, den MBR zu aktualisieren. Wenn die MBR-Sicherheit aktiviert ist, während Sie die Partitionierung oder Formatierung der Festplatte ändern, erhalten Sie beim nächsten Start oder Neustart des Computers möglicherweise Fehlermeldungen vom Festplattendienstprogramm oder einen Warnhinweis von MBR Security. Führen Sie die folgenden Schritte durch, um MBR Security zu deaktivieren:

1. Schalten Sie den Computer ein, oder starten Sie ihn neu. Klicken Sie in Windows auf **Start > Beenden > Neu starten**.
2. Drücken Sie die Taste **F10**, sobald die LED-Anzeige des Monitors grün aufleuchtet. Drücken Sie die **Eingabetaste**, um ggf. den Titelbildschirm zu überspringen.

Wenn Sie die Taste **F10** nicht zum richtigen Zeitpunkt drücken, müssen Sie den Computer aus- und wieder einschalten und dann die Taste **F10** erneut drücken, um das Dienstprogramm aufzurufen.

3. Wählen Sie **Security > Master Boot Record Security > Disabled** (Sicherheit > Master Boot Record-Sicherheit > Deaktiviert).
4. Klicken Sie zum Beenden auf **File (Datei) > Save Changes (Änderungen speichern)** und **Exit** (Schließen).

Kabelschloss

Die Anbringung eines Kabelschlosses ist auf der Rückseite des Computers möglich, so dass dieser an einem festen Gegenstand angeschlossen werden kann.

Anleitungen mit den entsprechenden Abbildungen finden Sie im *Hardware-Referenzhandbuch* auf der *Documentation Library* CD.

Fingerprint Identification Technology

Die HP Fingerprint Identification Technology macht die Eingabe eines Benutzerkennworts überflüssig, erhöht die Netzwerksicherheit, vereinfacht den Anmeldungsvorgang und verringert die mit dem Management von Firmennetzwerken verbundenen Kosten. Wegen ihres erschwinglichen Preises ist sie nicht mehr nur High-Tech-Organisationen mit hohem Sicherheitsbedürfnis vorbehalten.

Die Unterstützung für die Fingerprint Identification Technology hängt von dem jeweiligen Modell ab.

Weitere Informationen finden Sie unter folgender Adresse:

http://h18000.www1.hp.com/solutions/security.

Fehlermeldung und Fehlerbehebung

Die Funktionen zur Fehlermeldung und Fehlerbehebung sorgen durch die Kombination innovativer Hardware- und Softwaretechnologien dafür, dass der Verlust wichtiger Daten verhindert Ausfälle vermieden werden können.

Im Falle eines Fehlers gibt der Computer eine Warnmeldung aus, die den Fehler beschreibt und Vorsichtsmaßnahmen empfiehlt. Sie können sich dann den aktuellen Zustand des Systems über HP Client Manager anzeigen lassen. Wenn der Computer an ein Netzwerk angeschlossen ist, das von HP Insight Manager, HP Client Manager oder einem anderen Systemverwaltungsprogramm überwacht wird, sendet der Computer auch an die Netzwerk-Management-Anwendung eine Fehlermeldung.

Drive Protection System

Das Drive Protection System (DPS) ist ein in die Festplatten bestimmter HP Computer integriertes Diagnose-Tool. Dieses Tool soll die Diagnostizierung von Problemen unterstützen, die ein Austauschen der Festplatte erforderlich machen könnten.

Jede Festplatte wird vor dem Einbau in einen HP Computer unter Verwendung von DPS getestet, und wichtige Informationen werden permanent auf der Festplatte gespeichert. Die Testergebnisse werden bei jeder Ausführung von DPS auf der Festplatte gespeichert. Diese Informationen können dem Compaq Servicepartner bei der Diagnose von Zuständen nützlich sein, die Sie zur Ausführung der DPS-Software veranlasst haben. Hinweise zur Verwendung von DPS finden Sie im *Fehlerbeseitigungs-Handbuch*.

Überspannungsschutz

Ein integriertes überspannungstolerantes Netzteil bietet eine größere Zuverlässigkeit, wenn der Computer einer unvorhergesehen hohen Spannung ausgesetzt wird. Dieses Netzteil ist so ausgelegt, dass eine Überspannung von bis zu 2000 V ohne Systemausfall oder Datenverluste neutralisiert werden kann.

Thermosensor

Der Thermosensor ist eine Hard- und Softwarefunktion zur Messung der Innentemperatur eines Computers. Diese Funktion zeigt eine Warnmeldung an, wenn der normale Temperaturbereich überschritten wird, so dass Sie Maßnahmen ergreifen können, bevor die internen Komponenten beschädigt werden oder Daten verloren gehen.

Index